Network Working Group
Request for Comments: 2617
Obsoletes: 2069
Category: Standards Track

J. Franks
Northwestern University
P. Hallam-Baker
Verisign, Inc.
J. Hostetler
AbiSource, Inc.
S. Lawrence
Agranat Systems, Inc.
P. Leach
Microsoft Corporation
A. Luotonen
Netscape Communications Corporation
L. Stewart
Open Market, Inc.
June 1999

HTTP Authentication: Basic and Digest Access Authentication

Status of this Memo

Copyright Notice

Abstract

"HTTP/1.0", includes the specification for a Basic Access Authentication scheme. This scheme is not considered to be a secure method of user authentication (unless used in conjunction with some external secure system such as SSL [5]), as the user name and password are passed over the network as cleartext.

This document also provides the specification for HTTP's authentication framework, the original Basic authentication scheme and a scheme based on cryptographic hashes, referred to as "Digest Access Authentication". It is therefore also intended to serve as a replacement for RFC 2069 [6]. Some optional elements specified by RFC 2069 have been removed from this specification due to problems found since its publication; other new elements have been added for compatibility, those new elements have been made optional, but are strongly recommended.

Like Basic, Digest access authentication verifies that both parties to a communication know a shared secret (a password); unlike Basic, this verification can be done without sending the password in the clear, which is Basic's biggest weakness. As with most other

authentication protocols, the greatest sources of risks are usually found not in the core protocol itself but in policies and procedures surrounding its use.

Table of Contents

1 Access Authentication

1.1 Reliance on the HTTP/1.1 Specification

This specification is a companion to the HTTP/1.1 specification [2]. It uses the augmented BNF section 2.1 of that document, and relies on both the non-terminals defined in that document and other aspects of the HTTP/1.1 specification.

1.2 Access Authentication Framework

HTTP provides a simple challenge-response authentication mechanism that MAY be used by a server to challenge a client request and by a client to provide authentication information. It uses an extensible, case-insensitive token to identify the authentication scheme, followed by a comma-separated list of attribute-value pairs which carry the parameters necessary for achieving authentication via that scheme.

```
auth-scheme    = token
auth-param     = token "=" ( token | quoted-string )
```

The 401 (Unauthorized) response message is used by an origin server to challenge the authorization of a user agent. This response MUST include a WWW-Authenticate header field containing at least one challenge applicable to the requested resource. The 407 (Proxy Authentication Required) response message is used by a proxy to challenge the authorization of a client and MUST include a Proxy-Authenticate header field containing at least one challenge applicable to the proxy for the requested resource.

```
challenge   = auth-scheme 1*SP 1#auth-param
```

Note: User agents will need to take special care in parsing the WWW-Authenticate or Proxy-Authenticate header field value if it contains more than one challenge, or if more than one WWW-Authenticate header field is provided, since the contents of a challenge may itself contain a comma-separated list of authentication parameters.

The authentication parameter realm is defined for all authentication schemes:

```
realm       = "realm" "=" realm-value
realm-value = quoted-string
```


The realm directive (case-insensitive) is required for all authentication schemes that issue a challenge. The realm value (case-sensitive), in combination with the canonical root URL (the absoluteURI for the server whose abs_path is empty; see section 5.1.2 of [2]) of the server being accessed, defines the protection space. These realms allow the protected resources on a server to be partitioned into a set of protection spaces, each with its own authentication scheme and/or authorization database. The realm value is a string, generally assigned by the origin server, which may have additional semantics specific to the authentication scheme. Note that there may be multiple challenges with the same auth-scheme but different realms.

A user agent that wishes to authenticate itself with an origin server--usually, but not necessarily, after receiving a 401 (Unauthorized)--MAY do so by including an Authorization header field with the request. A client that wishes to authenticate itself with a proxy--usually, but not necessarily, after receiving a 407 (Proxy Authentication Required)--MAY do so by including a Proxy-Authorization header field with the request. Both the Authorization field value and the Proxy-Authorization field value consist of credentials containing the authentication information of the client for the realm of the resource being requested. The user agent MUST choose to use one of the challenges with the strongest auth-scheme it

understands and request credentials from the user based upon that challenge.

credentials = auth-scheme #auth-param

Note that many browsers will only recognize Basic and will require that it be the first auth-scheme presented. Servers should only include Basic if it is minimally acceptable.

The protection space determines the domain over which credentials can be automatically applied. If a prior request has been authorized, the same credentials MAY be reused for all other requests within that protection space for a period of time determined by the authentication scheme, parameters, and/or user preference. Unless otherwise defined by the authentication scheme, a single protection space cannot extend outside the scope of its server.

If the origin server does not wish to accept the credentials sent with a request, it SHOULD return a 401 (Unauthorized) response. The response MUST include a WWW-Authenticate header field containing at least one (possibly new) challenge applicable to the requested resource. If a proxy does not accept the credentials sent with a request, it SHOULD return a 407 (Proxy Authentication Required). The response MUST include a Proxy-Authenticate header field containing a

(possibly new) challenge applicable to the proxy for the requested resource.

The HTTP protocol does not restrict applications to this simple challenge-response mechanism for access authentication. Additional mechanisms MAY be used, such as encryption at the transport level or via message encapsulation, and with additional header fields specifying authentication information. However, these additional mechanisms are not defined by this specification.

Proxies MUST be completely transparent regarding user agent authentication by origin servers. That is, they must forward the WWW-Authenticate and Authorization headers untouched, and follow the rules found in section 14.8 of [2]. Both the Proxy-Authenticate and the Proxy-Authorization header fields are hop-by-hop headers (see section 13.5.1 of [2]).

2 Basic Authentication Scheme

The "basic" authentication scheme is based on the model that the client must authenticate itself with a user-ID and a password for each realm. The realm value should be considered an opaque string which can only be compared for equality with other realms on that server. The server will service the request only if it can validate the user-ID and password for the protection space of the Request-URI. There are no optional authentication parameters.

For Basic, the framework above is utilized as follows:

```
challenge   = "Basic" realm
credentials = "Basic" basic-credentials
```

Upon receipt of an unauthorized request for a URI within the protection space, the origin server MAY respond with a challenge like

the following:

```
WWW-Authenticate: Basic realm="WallyWorld"
```

where "WallyWorld" is the string assigned by the server to identify the protection space of the Request-URI. A proxy may respond with the same challenge using the Proxy-Authenticate header field.

To receive authorization, the client sends the userid and password, separated by a single colon (":") character, within a base64 [7] encoded string in the credentials.

```
basic-credentials = base64-user-pass
base64-user-pass  = <base64 [4] encoding of user-pass,
```



```
                    except not limited to 76 char/line>
user-pass   = userid ":" password
userid      = *<TEXT excluding ":">
password    = *TEXT
```

Userids might be case sensitive.

If the user agent wishes to send the userid "Aladdin" and password "open sesame", it would use the following header field:

```
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

A client SHOULD assume that all paths at or deeper than the depth of the last symbolic element in the path field of the Request-URI also are within the protection space specified by the Basic realm value of the current challenge. A client MAY preemptively send the corresponding Authorization header with requests for resources in that space without receipt of another challenge from the server. Similarly, when a client sends a request to a proxy, it may reuse a userid and password in the Proxy-Authorization header field without receiving another challenge from the proxy server. See section 4 for security considerations associated with Basic authentication.

3 Digest Access Authentication Scheme

3.1 Introduction

3.1.1 Purpose

The protocol referred to as "HTTP/1.0" includes the specification for a Basic Access Authentication scheme[1]. That scheme is not considered to be a secure method of user authentication, as the user name and password are passed over the network in an unencrypted form. This section provides the specification for a scheme that does not send the password in cleartext, referred to as "Digest Access Authentication".

The Digest Access Authentication scheme is not intended to be a complete answer to the need for security in the World Wide Web. This scheme provides no encryption of message content. The intent is simply to create an access authentication method that avoids the most serious flaws of Basic authentication.

3.1.2 Overall Operation

Like Basic Access Authentication, the Digest scheme is based on a simple challenge-response paradigm. The Digest scheme challenges using a nonce value. A valid response contains a checksum (by

default, the MD5 checksum) of the username, the password, the given nonce value, the HTTP method, and the requested URI. In this way, the password is never sent in the clear. Just as with the Basic scheme, the username and password must be prearranged in some fashion not addressed by this document.

3.1.3 Representation of digest values

An optional header allows the server to specify the algorithm used to create the checksum or digest. By default the MD5 algorithm is used and that is the only algorithm described in this document.

For the purposes of this document, an MD5 digest of 128 bits is represented as 32 ASCII printable characters. The bits in the 128 bit digest are converted from most significant to least significant bit, four bits at a time to their ASCII presentation as follows. Each four bits is represented by its familiar hexadecimal notation from the characters 0123456789abcdef. That is, binary 0000 gets represented by the character '0', 0001, by '1', and so on up to the representation of 1111 as 'f'.

3.1.4 Limitations

The Digest authentication scheme described in this document suffers from many known limitations. It is intended as a replacement for Basic authentication and nothing more. It is a password-based system and (on the server side) suffers from all the same problems of any password system. In particular, no provision is made in this protocol for the initial secure arrangement between user and server to establish the user's password.

Users and implementors should be aware that this protocol is not as secure as Kerberos, and not as secure as any client-side private-key scheme. Nevertheless it is better than nothing, better than what is commonly used with telnet and ftp, and better than Basic authentication.

3.2 Specification of Digest Headers

The Digest Access Authentication scheme is conceptually similar to the Basic scheme. The formats of the modified WWW-Authenticate header line and the Authorization header line are specified below. In addition, a new header, Authentication-Info, is specified.

3.2.1 The WWW-Authenticate Response Header

If a server receives a request for an access-protected object, and an acceptable Authorization header is not sent, the server responds with a "401 Unauthorized" status code, and a WWW-Authenticate header as per the framework defined above, which for the digest scheme is utilized as follows:

```
challenge        =  "Digest" digest-challenge

digest-challenge  = 1#( realm | [ domain ] | nonce |
                    [ opaque ] |[ stale ] | [ algorithm ] |
                    [ qop-options ] | [auth-param] )


domain            = "domain" "=" <"> URI ( 1*SP URI ) <">
URI               = absoluteURI | abs_path
nonce             = "nonce" "=" nonce-value
nonce-value       = quoted-string
opaque            = "opaque" "=" quoted-string
stale             = "stale" "=" ( "true" | "false" )
algorithm         = "algorithm" "=" ( "MD5" | "MD5-sess" |
                     token )
qop-options       = "qop" "=" <"> 1#qop-value <">
qop-value         = "auth" | "auth-int" | token
```

The meanings of the values of the directives used above are as follows:

realm
A string to be displayed to users so they know which username and password to use. This string should contain at least the name of the host performing the authentication and might additionally indicate the collection of users who might have access. An example might be "registered_users@gotham.news.com".

domain
A quoted, space-separated list of URIs, as specified in RFC XURI [7], that define the protection space. If a URI is an abs_path, it is relative to the canonical root URL (see section 1.2 above) of the server being accessed. An absoluteURI in this list may refer to a different server than the one being accessed. The client can use this list to determine the set of URIs for which the same authentication information may be sent: any URI that has a URI in this list as a prefix (after both have been made absolute) may be assumed to be in the same protection space. If this directive is omitted or its value is empty, the client should assume that the protection space consists of all URIs on the responding server.

This directive is not meaningful in Proxy-Authenticate headers, for which the protection space is always the entire proxy; if present it should be ignored.

nonce
A server-specified data string which should be uniquely generated each time a 401 response is made. It is recommended that this string be base64 or hexadecimal data. Specifically, since the

string is passed in the header lines as a quoted string, the double-quote character is not allowed.

The contents of the nonce are implementation dependent. The quality of the implementation depends on a good choice. A nonce might, for example, be constructed as the base 64 encoding of

    time-stamp H(time-stamp ":" ETag ":" private-key)

where time-stamp is a server-generated time or other non-repeating value, ETag is the value of the HTTP ETag header associated with the requested entity, and private-key is data known only to the server. With a nonce of this form a server would recalculate the hash portion after receiving the client authentication header and reject the request if it did not match the nonce from that header or if the time-stamp value is not recent enough. In this way the server can limit the time of the nonce's validity. The inclusion of the ETag prevents a replay request for an updated version of the resource. (Note: including the IP address of the client in the nonce would appear to offer the server the ability to limit the reuse of the nonce to the same client that originally got it. However, that would break proxy farms, where requests from a single user often go through different proxies in the farm. Also, IP address spoofing is not that hard.)

An implementation might choose not to accept a previously used nonce or a previously used digest, in order to protect against a replay attack. Or, an implementation might choose to use one-time nonces or digests for POST or PUT requests and a time-stamp for GET requests. For more details on the issues involved see section 4. of this document.

The nonce is opaque to the client.

opaque
A string of data, specified by the server, which should be returned by the client unchanged in the Authorization header of subsequent requests with URIs in the same protection space. It is recommended that this string be base64 or hexadecimal data.

stale
A flag, indicating that the previous request from the client was rejected because the nonce value was stale. If stale is TRUE (case-insensitive), the client may wish to simply retry the request with a new encrypted response, without reprompting the user for a new username and password. The server should only set stale to TRUE if it receives a request for which the nonce is invalid but with a valid digest for that nonce (indicating that the client knows the correct username/password). If stale is FALSE, or anything other than TRUE, or the stale directive is not present, the username and/or password are invalid, and new values must be obtained.

algorithm
A string indicating a pair of algorithms used to produce the digest and a checksum. If this is not present it is assumed to be "MD5". If the algorithm is not understood, the challenge should be ignored (and a different one used, if there is more than one).

In this document the string obtained by applying the digest algorithm to the data "data" with secret "secret" will be denoted by KD(secret, data), and the string obtained by applying the checksum algorithm to the data "data" will be denoted H(data). The notation unq(X) means the value of the quoted-string X without the surrounding quotes.

For the "MD5" and "MD5-sess" algorithms

```
H(data) = MD5(data)
```

and

```
KD(secret, data) = H(concat(secret, ":", data))
```

i.e., the digest is the MD5 of the secret concatenated with a colon concatenated with the data. The "MD5-sess" algorithm is intended to allow efficient 3rd party authentication servers; for the difference in usage, see the description in section 3.2.2.2.

qop-options
This directive is optional, but is made so only for backward compatibility with RFC 2069 [6]; it SHOULD be used by all implementations compliant with this version of the Digest scheme. If present, it is a quoted string of one or more tokens indicating the "quality of protection" values supported by the server. The value "auth" indicates authentication; the value "auth-int" indicates authentication with integrity protection; see the

descriptions below for calculating the response directive value for the application of this choice. Unrecognized options MUST be ignored.

auth-param
This directive allows for future extensions. Any unrecognized directive MUST be ignored.

3.2.2 The Authorization Request Header

The client is expected to retry the request, passing an Authorization header line, which is defined according to the framework above, utilized as follows.

```
credentials      = "Digest" digest-response
digest-response  = 1#( username | realm | nonce | digest-uri
                | response | [ algorithm ] | [cnonce] |
                [opaque] | [message-qop] |
                    [nonce-count]  | [auth-param] )

username         = "username" "=" username-value
username-value   = quoted-string
digest-uri       = "uri" "=" digest-uri-value
digest-uri-value = request-uri   ; As specified by HTTP/1.1
message-qop      = "qop" "=" qop-value
cnonce           = "cnonce" "=" cnonce-value
cnonce-value     = nonce-value
nonce-count      = "nc" "=" nc-value
```

```
nc-value         = 8LHEX
response         = "response" "=" request-digest
request-digest = <"> 32LHEX <">
LHEX             =  "0" | "1" | "2" | "3" |
                    "4" | "5" | "6" | "7" |
                    "8" | "9" | "a" | "b" |
                    "c" | "d" | "e" | "f"
```

The values of the opaque and algorithm fields must be those supplied in the WWW-Authenticate response header for the entity being requested.

response
A string of 32 hex digits computed as defined below, which proves that the user knows a password

username
The user's name in the specified realm.

digest-uri
The URI from Request-URI of the Request-Line; duplicated here because proxies are allowed to change the Request-Line in transit.

qop
Indicates what "quality of protection" the client has applied to the message. If present, its value MUST be one of the alternatives the server indicated it supports in the WWW-Authenticate header. These values affect the computation of the request-digest. Note that this is a single token, not a quoted list of alternatives as in WWW- Authenticate. This directive is optional in order to preserve backward compatibility with a minimal implementation of RFC 2069 [6], but SHOULD be used if the server indicated that qop is supported by providing a qop directive in the WWW-Authenticate header field.

cnonce
This MUST be specified if a qop directive is sent (see above), and MUST NOT be specified if the server did not send a qop directive in the WWW-Authenticate header field. The cnonce-value is an opaque quoted string value provided by the client and used by both client and server to avoid chosen plaintext attacks, to provide mutual authentication, and to provide some message integrity protection. See the descriptions below of the calculation of the response-digest and request-digest values.

nonce-count
This MUST be specified if a qop directive is sent (see above), and MUST NOT be specified if the server did not send a qop directive in the WWW-Authenticate header field. The nc-value is the hexadecimal count of the number of requests (including the current request) that the client has sent with the nonce value in this request. For example, in the first request sent in response to a given nonce value, the client sends "nc=00000001". The purpose of this directive is to allow the server to detect request replays by maintaining its own copy of this count - if the same nc-value is seen twice, then the request is a replay. See the description below of the construction of the request-digest value.

auth-param
  This directive allows for future extensions. Any unrecognized
  directive MUST be ignored.

If a directive or its value is improper, or required directives are missing, the proper response is 400 Bad Request. If the request-digest is invalid, then a login failure should be logged, since repeated login failures from a single client may indicate an attacker attempting to guess passwords.

The definition of request-digest above indicates the encoding for its value. The following definitions show how the value is computed.

3.2.2.1 Request-Digest

If the "qop" value is "auth" or "auth-int":

```
request-digest  = <"> < KD ( H(A1),     unq(nonce-value)
                                      ":" nc-value
                                      ":" unq(cnonce-value)
                                      ":" unq(qop-value)
                                      ":" H(A2)
                            ) <">
```

If the "qop" directive is not present (this construction is for compatibility with RFC 2069):

```
request-digest  =
            <"> < KD ( H(A1), unq(nonce-value) ":" H(A2) ) >
<">
```

See below for the definitions for A1 and A2.

3.2.2.2 A1

If the "algorithm" directive's value is "MD5" or is unspecified, then A1 is:

```
A1       = unq(username-value) ":" unq(realm-value) ":" passwd
```

where

```
passwd   = < us
```

[Sip-implementors] RE: www-authenticate header

Jonathan Rosenberg jdrosen@dynamicsoft.com
Mon, 4 Jun 2001 12:23:41 -0400

- Previous message: [Sip-implementors] RE: www-authenticate header
- Next message: [Sip-implementors] (no subject)
- **Messages sorted by:** [date] [thread] [subject] [author]

> *-----Original Message-----*
> *From: aki.niemi@nokia.com [mailto:aki.niemi@nokia.com]*
> *Sent: Monday, June 04, 2001 9:02 AM*
> *To: jdrosen@dynamicsoft.com*
> *Cc: sunilk@netbrahma.com; sip-implementors@cs.columbia.edu*
> *Subject: RE: [Sip-implementors] RE: www-authenticate header*
>
>
> *Hi,*
>
> *A quick question below...*
>
> *> > -----Original Message-----*
> *> > From: T.Sunil Kumar [mailto:sunilk@netbrahma.com]*
> *> > Sent: Thursday, May 17, 2001 9:14 AM*
> *> > To: SIP implementors; Jonathan Rosenberg*
> *> > Subject: www-authenticate header*
> *> >*
> *> >*
> *> > Hi,*
> *> >*
> *> > Should it be treated as 401 response header alone or*
> *request header*
> *> > also?*
> *> >*
> *> > It used to be both request and response, since we used to support*
> *> > authentication of responses by "mirroring" the request*
> *authentication*
> *> > mechanism. However, rfc2617 supports a mechanism for response*
> *> > authentication*
> *> > that is now to be used instead. THerefore, WWW-AUthenticate*
> *> > should just be a*
> *> > request header.*
> *> >*
> *> > This will be reflected in the next rev.*
>
> *This sounds good. Just for clarification, is this to say that*
> *the RFC 2617*
> *style authentication-info headers will be added to the next SIP bis?*

Yes. This was too big a change for -03, as I wanted to get that out the door finally. It will therefore come in -04.

-Jonathan R.

Network Working Group
Request for Comments: 3261
Obsoletes: 2543
Category: Standards Track

J. Rosenberg
dynamicsoft
H. Schulzrinne
Columbia U.
G. Camarillo
Ericsson
A. Johnston
WorldCom
J. Peterson
Neustar
R. Sparks
dynamicsoft
M. Handley
ICIR
E. Schooler
AT&T
June 2002

SIP: Session Initiation Protocol

Status of this Memo

Copyright Notice

Abstract

This document describes Session Initiation Protocol (SIP), an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.

SIP invitations used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types. SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP also provides a registration function that allows users to upload their current locations for use by proxy servers. SIP runs on top of several different transport protocols.

Table of Contents

request. A mandatory response header field MUST be present in the response, and the header field MUST be understood by the UAC processing the response. "Not applicable" means that the header field MUST NOT be present in a request. If one is placed in a request by mistake, it MUST be ignored by the UAS receiving the request. Similarly, a header field labeled "not applicable" for a response means that the UAS MUST NOT place the header field in the response, and the UAC MUST ignore the header field in the response.

A UA SHOULD ignore extension header parameters that are not understood.

A compact form of some common header field names is also defined for use when overall message size is an issue.

The Contact, From, and To header fields contain a URI. If the URI contains a comma, question mark or semicolon, the URI MUST be enclosed in angle brackets (< and >). Any URI parameters are contained within these brackets. If the URI is not enclosed in angle brackets, any semicolon-delimited parameters are header-parameters, not URI parameters.

20.1 Accept

The Accept header field follows the syntax defined in [H14.1]. The semantics are also identical, with the exception that if no Accept header field is present, the server SHOULD assume a default value of application/sdp.

An empty Accept header field means that no formats are acceptable.

Example:

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
Accept	R		-	o	-	o	m*	o
Accept	2xx		-	-	-	o	m*	o
Accept	415		-	c	-	c	c	c
Accept-Encoding	R		-	o	-	o	o	o
Accept-Encoding	2xx		-	-	-	o	m*	o
Accept-Encoding	415		-	c	-	c	c	c
Accept-Language	R		-	o	-	o	o	o
Accept-Language	2xx		-	-	-	o	m*	o
Accept-Language	415		-	c	-	c	c	c
Alert-Info	R	ar	-	-	-	o	-	-
Alert-Info	180	ar	-	-	-	o	-	-
Allow	R		-	o	-	o	o	o
Allow	2xx		-	o	-	m*	m*	o
Allow	r		-	o	-	o	o	o
Allow	405		-	m	-	m	m	m
Authentication-Info	2xx		-	o	-	o	o	o

Authorization	R		o	o	o	o	o	o
Call-ID	c	r	m	m	m	m	m	m
Call-Info		ar	-	-	-	o	o	o
Contact	R		o	-	-	m	o	o
Contact	1xx		-	-	-	o	-	-
Contact	2xx		-	-	-	m	o	o
Contact	3xx	d	-	o	-	o	o	o
Contact	485		-	o	-	o	o	o
Content-Disposition			o	o	-	o	o	o
Content-Encoding			o	o	-	o	o	o
Content-Language			o	o	-	o	o	o
Content-Length		ar	t	t	t	t	t	t
Content-Type			*	*	-	*	*	*
CSeq	c	r	m	m	m	m	m	m
Date		a	o	o	o	o	o	o
Error-Info	300-699	a	-	o	o	o	o	o
Expires			-	-	-	o	-	o
From	c	r	m	m	m	m	m	m
In-Reply-To	R		-	-	-	o	-	-
Max-Forwards	R	amr	m	m	m	m	m	m
Min-Expires	423		-	-	-	-	-	m
MIME-Version			o	o	-	o	o	o
Organization		ar	-	-	-	o	o	o

Table 2: Summary of header fields, A--O

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
Priority	R	ar	-	-	-	o	-	-
Proxy-Authenticate	407	ar	-	m	-	m	m	m
Proxy-Authenticate	401	ar	-	o	o	o	o	o
Proxy-Authorization	R	dr	o	o	-	o	o	o
Proxy-Require	R	ar	-	o	-	o	o	o
Record-Route	R	ar	o	o	o	o	o	-
Record-Route	2xx,18x	mr	-	o	o	o	o	-
Reply-To			-	-	-	o	-	-
Require		ar	-	c	-	c	c	c
Retry-After	404,413,480,486		-	o	o	o	o	o
	500,503		-	o	o	o	o	o
	600,603		-	o	o	o	o	o
Route	R	adr	c	c	c	c	c	c
Server	r		-	o	o	o	o	o
Subject	R		-	-	-	o	-	-
Supported	R		-	o	o	m*	o	o
Supported	2xx		-	o	o	m*	m*	o
Timestamp			o	o	o	o	o	o
To	c(1)	r	m	m	m	m	m	m
Unsupported	420		-	m	-	m	m	m
User-Agent			o	o	o	o	o	o
Via	R	amr	m	m	m	m	m	m
Via	rc	dr	m	m	m	m	m	m
Warning	r		-	o	o	o	o	o
WWW-Authenticate	401	ar	-	m	-	m	m	m
WWW-Authenticate	407	ar	-	o	-	o	o	o

Table 3: Summary of header fields, P--Z; (1): copied with possible

This helps prevent disruptions that could result from the use of this header field by untrusted elements.

Example:

```
Alert-Info: <http://www.example.com/sounds/moo.wav>
```


20.5 Allow

The Allow header field lists the set of methods supported by the UA generating the message.

All methods, including ACK and CANCEL, understood by the UA MUST be included in the list of methods in the Allow header field, when present. The absence of an Allow header field MUST NOT be interpreted to mean that the UA sending the message supports no methods. Rather, it implies that the UA is not providing any information on what methods it supports.

Supplying an Allow header field in responses to methods other than OPTIONS reduces the number of messages needed.

Example:

```
Allow: INVITE, ACK, OPTIONS, CANCEL, BYE
```

20.6 Authentication-Info

The Authentication-Info header field provides for mutual authentication with HTTP Digest. A UAS MAY include this header field in a 2xx response to a request that was successfully authenticated using digest based on the Authorization header field.

Syntax and semantics follow those specified in RFC 2617 [17].

Example:

```
Authentication-Info: nextnonce="47364c23432d2e131a5fb210812c"
```

20.7 Authorization

The Authorization header field contains authentication credentials of a UA. Section 22.2 overviews the use of the Authorization header field, and Section 22.4 describes the syntax and semantics when used with HTTP authentication.

This header field, along with Proxy-Authorization, breaks the general rules about multiple header field values. Although not a comma-separated list, this header field name may be present multiple times, and MUST NOT be combined into a single header line using the usual rules described in Section 7.3.

2279, January 1998.

[8] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[9] Vaha-Sipila, A., "URLs for Telephone Calls", RFC 2806, April 2000.

[10] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[11] Freed, F. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996.

[12] Eastlake, D., Crocker, S. and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

[13] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with SDP", RFC 3264, June 2002.

[14] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[15] Postel, J., "DoD Standard Transmission Control Protocol", RFC 761, January 1980.

[16] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L. and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

[17] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A. and L. Stewart, "HTTP authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[18] Troost, R., Dorner, S. and K. Moore, "Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field", RFC 2183, August 1997.

[19] Zimmerer, E., Peterson, J., Vemuri, A., Ong, L., Audet, F., Watson, M. and M. Zonoun, "MIME media types for ISUP and QSIG Objects", RFC 3204, December 2001.

[20] Braden, R., "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, October 1989.

[21] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, January 1998.

[22] Galvin, J., Murphy, S., Crocker, S. and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, October 1995.

[23] Housley, R., "Cryptographic Message Syntax", RFC 2630, June 1999.

[24] Ramsdell B., "S/MIME Version 3 Message Specification", RFC 2633,

File 347:JAPIO Nov 1976-2004/Oct(Updated 050209)
(c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200516
(c) 2005 Thomson Derwent

Set	Items	Description
S1	1239	SIP OR SESSION()(INITIATION OR INITIATED)()PROTOCOL
S2	47	INVITE(1W)(REQUEST? ? OR MESSAGE? ?)
S3	0	S2(10N)AUTHENTICAT?
S4	34	S1 AND S2
S5	3	S4 AND AUTHENTICAT?

5/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2005 JPO & JAPIO. All rts. reserv.

07614680 **Image available**
METHOD AND SYSTEM FOR INCORPORATING SECURITY MECHANISM INTO **SESSION INITIATION PROTOCOL** REQUEST MESSAGE FOR CLIENT PROXY **AUTHENTICATION**

PUB. NO.: 2003-108527 [JP 2003108527 A]
PUBLISHED: April 11, 2003 (20030411)
INVENTOR(s): BOBDE NIKHIL P
DEMIRTJIS ANN
HAN MU
APPLICANT(s): MICROSOFT CORP
APPL. NO.: 2002-174951 [JP 2002174951]
FILED: June 14, 2002 (20020614)
PRIORITY: 01 298239 [US 2001298239], US (United States of America), June 14, 2001 (20010614)
02 151747 [US 2002151747], US (United States of America), May 17, 2002 (20020517)
INTL CLASS: G06F-015/00; G09C-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To provide a method and a system for allowing an **SIP** client and an **SIP** proxy to **authenticate** each other by incorporating a Cerberus security mechanism into a message flow of signaling operation based on a **session initiation protocol** .

SOLUTION: When receiving a request message such as an **INVITE request** from the **SIP** client, the **SIP** proxy sends a challenge message for indicating the necessity of **authentication** based on Cerberus in response to this message. The **SIP** client sends a second request message having a proxy authorization header including **authenticating** data including a Cerberus server ticket to a proxy in response to this message so that the proxy can **authenticate** a user of the client.

5/5/2 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005 Thomson Derwent. All rts. reserv.

016081418 **Image available**
WPI Acc No: 2004-239279/200422
XRPX Acc No: N04-189646
Conferencing resource administering method, for wireless communication system, involves allocating network address identifying resource capable of sustaining conference call
Patent Assignee: NOKIA CORP (OYNO); NIEMI A (NIEM-I)
Inventor: NIEMI A
Number of Countries: 105 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200421655	A1	20040311	WO 2003IB3813	A	20030815	200422 B
US 20040137887	A1	20040715	US 2003645848	A	20030822	200447
AU 2003256000	A1	20040319	AU 2003256000	A	20030815	200462

Priority Applications (No Type Date): GB 200219947 A 20020828
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200421655	A1	E	21	H04L-012/66	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW

Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT RO SD SE SI SK SL SZ TR TZ UG ZM ZW
US 20040137887 A1 H04M-003/42
AU 2003256000 A1 H04L-012/66 Based on patent WO 200421655

Abstract (Basic): WO 200421655 A1

NOVELTY - A message (21) requesting a resource capable of sustaining a conference call, is transmitted from a first terminal (10) to a server (12). The server allocates a network address identifying the resource (13) capable of sustaining the conference call. A second message comprising the network address is transmitted to the first terminal by the server. Preferably the first terminal transmits a third message comprising the network address to at least one other terminal.

DETAILED DESCRIPTION - In the case of a 3G network, the first terminal (user agent, 10) sends an **SIP INVITE message** (21) to a well known uniform resource identifier (URI), the message including details of the type of conference required, such as a preferred data rate. The user agent may then be sent an **SIP** message including an **authentication** challenge. Once **authenticated** , the server allocates a dynamic URI which identifies a resource that is available to handle a conference call, to which the network will route communications directed to that address. The server preferably allocates addresses for conferencing that refer to the resource. The dynamic URI is transmitted to the first user agent by the server in an **SIP** message (22), which is preferably a redirection message. The user agent then transmits an **INVITE message** (23) to the URI which acknowledges it, the user agent then referring the allocated URI to a second user agent (11), which in turn send a request message, such as an **INVITE message** (27), to the resource. Once the resource acknowledges this message the server and resource are able to communicate with each other.

INDEPENDENT CLAIMS are also included for the following:
(1) conference server; and
(2) communication system.

USE - For setting up conference calls, especially in a wireless communication system, e.g. using **SIP** signaling in a 3G IMS network.

ADVANTAGE - Allows use of standard **SIP** messages in the establishment of a conference call and does not require significant user configuration in the allocation of conferencing resources. Allows conferences to be set up without prearrangement. Prevents the problem of overlapping conference sessions, by the unique address provided to a particular conference at a time.

DESCRIPTION OF DRAWING(S) - The figure is a block diagram of a conferencing system according to the invention.

user agent (10,11)
server (12)
INVITE message (21)
SIP message (22)
pp; 21 DwgNo 3/3

Title Terms: RESOURCE; ADMINISTER; METHOD; WIRELESS; COMMUNICATE; SYSTEM; ALLOCATE; NETWORK; ADDRESS; IDENTIFY; RESOURCE; CAPABLE; SUSTAINED; CONFER; CALL
Derwent Class: W01; W02
International Patent Class (Main): H04L-012/66; H04M-003/42
International Patent Class (Additional): H04L-012/16; H04L-012/28; H04M-003/56; H04Q-007/38
File Segment: EPI

5/5/3 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014436714 **Image available**
WPI Acc No: 2002-257417/200230
XRPX Acc No: N02-199299
Performing universal mobile telephone service authentication **using** session initiation protocol **messages by forwarding** session

initiation protocol **requests from user agent to server**
Patent Assignee: NOKIA CORP (OYNO)
Inventor: FACCIN S; LE F; WOLFNER G
Number of Countries: 096 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200211469	A2	20020207	WO 2001US23764	A	20010730	200230	B
AU 200178057	A	20020213	AU 200178057	A	20010730	200238	
EP 1305911	A2	20030502	EP 2001956016	A	20010730	200331	
			WO 2001US23764	A	20010730		
KR 2003029805	A	20030416	KR 2003701503	A	20030130	200353	
BR 200112894	A	20031021	BR 200112894	A	20010730	200379	
			WO 2001US23764	A	20010730		
JP 2004505570	W	20040219	WO 2001US23764	A	20010730	200414	
			JP 2002515860	A	20010730		
MX 2003000960	A1	20030601	WO 2001US23764	A	20010730	200417	
			MX 2003960	A	20030131		
CN 1483265	A	20040317	CN 2001813612	A	20010730	200437	

Priority Applications (No Type Date): US 2000630425 A 20000801
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200211469	A2	E	13	H04Q-007/00	
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW					
AU 200178057	A			H04Q-007/00	Based on patent WO 200211469
EP 1305911	A2	E		H04L-012/28	Based on patent WO 200211469
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR					
KR 2003029805	A			H04Q-007/38	
BR 200112894	A			H04Q-007/00	Based on patent WO 200211469
JP 2004505570	W		25	H04Q-007/38	Based on patent WO 200211469
MX 2003000960	A1			H04Q-007/00	Based on patent WO 200211469
CN 1483265	A			H04L-012/28	

Abstract (Basic): WO 200211469 A2

NOVELTY - When a universal mobile telephone service **authentication** and key agreement needs to be performed at call set up or registration, the user agent in the user equipment sends a register or **invite request** to the call state control function, which can accept with an OK message (200) or ask for authorization with an unauthorized response (401), including a header field containing the requested authorization scheme and related parameters. The user agent may then send a new register or **invite request** with the appropriate authorization information.

DETAILED DESCRIPTION - AN INDEPENDENT CLAIM is included for a machine readable program storage device with instructions.

USE - Performing universal mobile telephone service **authentication** using **session initiation protocol** messages.

ADVANTAGE - Providing **authentication** by reusing and adapting existing mode.

DESCRIPTION OF DRAWING(S) - The drawing shows the data flow

OK message (200)

Unauthorized response (401)

pp; 13 DwgNo 1/2

File 348:EUROPEAN PATENTS 1978-2005/Feb W04
(c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20050303,UT=20050224
(c) 2005 WIPO/Univentio

Set	Items	Description
S1	5934	SIP OR SESSION()(INITIATION OR INITIATED)()PROTOCOL
S2	518	INVITE(1W)(REQUEST? ? OR MESSAGE? ?)
S3	15	S2(10N)AUTHENTICAT?

3/3,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01516001
Method and system for integrating security mechanisms into session initiation protocol request messages for client-proxy authentication
Verfahren und System zur Integration von Sicherheitsmechanismus in SIP Nachrichten fur Client-Proxy Authentifizierung
Dispositif et procede pour l'integration de mecanismes de securite dans les messages de requete SIP pour l'authentification client-proxy
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
Bobde, Nikhil P., 14405 43rd Place, Bellvue, Washington 98052, (US)
Demirtjis, Ann, 14811 NE 67th Street, Redmond, Washington 98052, (US)
Han, Mu, 7204 153rd Avenue NE, Redmond, Washington 98052, (US)
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721), Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1267548 A2 021218 (Basic)
APPLICATION (CC, No, Date): EP 2002013408 020612;
PRIORITY (CC, No, Date): US 298239 P 010614; US 151747 020517
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-029/06
ABSTRACT WORD COUNT: 104
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200251	1456
SPEC A	(English)	200251	7820
Total word count - document A			9276
Total word count - document B			0
Total word count - documents A + B			9276

...SPECIFICATION Layer (SSL) protocol. It will be appreciated that although in this example the SIP request is an **INVITE request** , the **authentication** scheme described below can also be used for other types of SIP requests, such as REGISTER, MESSAGE...

...SIP client 72 receives the 407 message 96 from the proxy server 74 in response to the **INVITE message** 82, it decides from the Proxy-**Authenticate** header 98 that the proxy server requires authentication of the user by means of the Kerberos mechanism...

...long-term key shared with the KDC 100. If the ticket is valid, the user 76 is **authenticated** , and the SIP proxy server 74 forwards the **INVITE message** 110 to the next proxy 120 on the signaling path. If the client 72 has requested mutual **authentication** in the Proxy-Authorization header 112 of the **INVITE message** 110, the proxy server 74 will sign future packets from the server to the client using a...

...Information header 124 that contains the credentials of the proxy 74 to allow the client 72 to **authenticate** the proxy.
Ultimately, the **INVITE message** 110 reaches the callee, i.e., the SIP client 86 of Bob's computer 88. If the...

...server 74 wants to challenge the identity of the SIP client (or its user) that sent an **INVITE message** , it sends a 407 message with a Proxy- **Authenticate** header back to the client. The syntax of Proxy-Authenticate header in a preferred embodiment requiring the...the signaling processing are shown. The SIP proxy server 74 has been

configured to require that all **INVITE requests** be **authenticated** for calls made to the Microsoft.com user name space. As a result, the SIP proxy server...in additional to the outbound proxy server 74 of the SIP client, and both proxies require client **authentication** before forwarding the **INVITE message** . In this case, the client 72 first goes through the same process as described above in connection...

...above, in a preferred embodiment the NTLM security mechanism can be optionally used for the client-proxy **authentication** . In this case, the client first sends an **INVITE message** 220 without **authentication** data, and the proxy returns a 407 message. The Proxy Authenticate header of this 407 message 222...data about the proxy. Based on the authentication data in the "200 OK" message 232, the client **authenticates** the proxy, and then sends out another **INVITE message** 236. Exemplary messages for this process are provided below.
FIG. 9 shows a scenario of NTLM-based...

...the security association with the proxy. The proxy then returns a "200 OK" message 246 with Proxy **Authentication** Information. After **authenticating** the proxy, the client sends a second **INVITE message** 248 to the proxy. Exemplary messages for this process are provided below.

In view of the many...

...CLAIMS message.
17. A method as in claim 16, wherein the first and second request messages are SIP **INVITE requests** .
18. A method as in claim 16, wherein the **authentication** data in the proxy-authorization header in the second request message include data requesting mutual authentication between...

3/3,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01295067
Methods and systems for internet protocol (IP) network surveillance
Verfahren und Vorrichtungen zur Uberwachung eines Internetprotokollnetzwerk es
Procedes et systemes de surveillance d'un reseau a protocole Internet
PATENT ASSIGNEE:
Nortel Networks Limited, (3029042), 2351 Boulevard Alfred-Nobel, St. Laurent, Quebec H4S 2A9, (CA), (Applicant designated States: all)
INVENTOR:
Fortman, Peter A., 9800 Rockledge Drive, Raleigh, North Carolina 27613, (US)
LEGAL REPRESENTATIVE:
Mackenzie, Andrew Bryan et al (79993), Sommerville & Rushton, 45 Grosvenor Road, St Albans, Herts. AL1 3AW, (GB)
PATENT (CC, No, Kind, Date): EP 1111892 A2 010627 (Basic)
EP 1111892 A3 031105
APPLICATION (CC, No, Date): EP 2000311068 001212;
PRIORITY (CC, No, Date): US 472377 991223
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04M-007/00; H04L-029/06; H04M-003/22
ABSTRACT WORD COUNT: 157
NOTE:
Figure number on first page: 2

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200126	2210
SPEC A	(English)	200126	11829
Total word count - document A			14039
Total word count - document B			0

Total word count - documents A + B 14039

...SPECIFICATION for an end user under.
Referring again to Figure 7(b), in line 6, after receiving the **INVITE message** , proxy server 710 contacts **authentication** server 706 (illustrated in Figure 7(a)) to authenticate end user device 700 and end user device...

3/3,K/3 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

01037803 **Image available**
PACKET-BASED CONVERSATIONAL SERVICE FOR A MULTIMEDIA SESSION IN A MOBILE COMMUNICATIONS SYSTEM
SERVICE CONVERSATIONNEL FONDE SUR LA COMMUTATION PAR PAQUETS POUR UNE SESSION MULTIMEDIA DANS UN SYSTEME DE COMMUNICATION MOBILE
Patent Applicant/Assignee:
TELEFONAKTIEBOLAGET LM ERICSSON (Publ), S-126 25 Stockholm, SE, SE (Residence), SE (Nationality)
Inventor(s):
BERGENLID Lars Herbert, Rayvagen 42, S-191 63 Sollentuna, SE,
OLSSON Magnus, Smabjorksvagen 47, S-163 42 Spanga, SE,
Legal Representative:
MONICA MAGNUSSON (agent), Ericsson AB, Patent Unit Radio Networks, S-164 80 Stockholm, SE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200367832 A1 20030814 (WO 0367832)
Application: WO 2003SE215 20030207 (PCT/WO SE0300215)
Priority Application: US 2002354483 20020208; US 2003347501 20030121
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 7316

Fulltext Availability:
Detailed Description

Detailed Description
... session details regarding the number of media flows and requested corresponding quality of io service. The IMS **authenticates** N91 as a subscriber and authorizes the session. The SIP **INVITE message** is forwarded to MT2 via external networks. MT2 confirms the session request in a SIP "183" Progress...

3/3,K/4 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00994033 **Image available**
ARCHITECTURE FOR TRANSPORTING PBX SIGNALING CODES VIA SIP
ARCHITECTURE UTILISANT UN SIP POUR ACHEMINER DES CODES DE SIGNALISATION PBX
Patent Applicant/Assignee:
ALCATEL INTERNETWORKING INC, 26801 West Agoura Road, Calabasas, CA 91301, US, US (Residence), US (Nationality)

Inventor(s):
WENGROVITZ Michael, 1315 Old Marlboro Road, Concord, MA 01742, US,
Legal Representative:
CHANG Josephine E (agent), Christie, Parker & Hale, LLP, P.O. Box 7068, Pasadena, CA 91109-7068, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200324062 A2-A3 20030320 (WO 0324062)
Application: WO 2002US28191 20020904 (PCT/WO US0228191)
Priority Application: US 2001317673 20010906; US 2001317744 20010906; US 200274340 20020212
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
CN JP
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
Publication Language: English
Filing Language: English
Fulltext Word Count: 8181

Fulltext Availability:
Detailed Description

Detailed Description
... invention, the PBX translator 30 verifies whether the 5 caller is an authorized caller by examining the **authentication** information in the body of the **INVITE** **message** . Alternatively, the PBX translator 30 does not necessarily require **authentication** for initiating a call through the translator.

If the caller is authenticated or no authentication is necessary...

3/3,K/5 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00977535 **Image available**
SYSTEM AND METHOD FOR EXTENDED SIP HEADERS FOR CDMA PARAMETERS
SYSTEME ET PROCEDE POUR ENTETES SIP ETENDUES DESTINEES A DES PARAMETRES AMRC
Patent Applicant/Assignee:
QUALCOMM INCORPORATED, 5775 Morehouse Drive, San Diego, CA 92121, US, US (Residence), US (Nationality)
Inventor(s):
VASSILOVSKI Dan, 715 Stratford Court, Del Mar, CA 92014, US,
DALEY Robert S, 766 Hoska Drive, Del Mar, CA 92014, US,
MARSHALL Maria, 2286 Fuerte Street, Oceanside, CA 92054, US,
Legal Representative:
WADSWORTH Philip R (et al) (agent), Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200307579 A2-A3 20030123 (WO 0307579)
Application: WO 2002US21934 20020712 (PCT/WO US0221934)
Priority Application: US 2001905510 20010713
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI
SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 6422

Fulltext Availability:
Detailed Description

Detailed Description
... The SIP Invite uses the originating wireless endpoint's full CDMA address for, e.g., authentication. Once **authentication** is successful, the originating EP endpoint reformulates the original SIP **Invite request** to address the destination party directly, but using only the SIP URL information corresponding to the originating...
...message contains some CDMA-specific parameters that are not required for SIP VOEP communication, while subsequent to **authentication** the second SEP **Invite message** contains only parameters that are required for SEP VOIP communication and that consequently excludes CDMA-specific parameters...

3/3,K/6 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00977529 **Image available**
A MECHANISM TO ALLOW AUTHENTICATION OF SIP CALLS TERMINATED TO A MOBILE NODE
MECANISME PERMETTANT L'AUTHENTIFICATION D'APPELS SIP ABOUTISSANT SUR UN NOEUD MOBILE
Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
FACCIN Stefano, 3421 Dartmoor Drive, Dallas, TX 75229-2622, US, US (Residence), IT (Nationality), (Designated only for: US)
LE Franck, 2715 West Royal Lane, Irving, TX 75063, US, US (Residence), FR (Nationality), (Designated only for: US)
Legal Representative:
LESON Thomas Johannes Alois (et al) (agent), TBK-Patent, Bavariaring 4-6, 80336 Munchen, DE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200307573 A1 20030123 (WO 0307573)
Application: WO 2002IB2718 20020711 (PCT/WO IB0202718)
Priority Application: US 2001905463 20010713
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI
SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 7613

Fulltext Availability:
Detailed Description
Claims

Detailed Description
... may be adopted as a control protocol. For example, the session invitation message may be a SIP **INVITE request** including an **authentication** header field. The response message may be a SIP response message including an authorization header field.

The...present embodiment, an additional field,

i.e., an additional parameter has to be included into the SIP **INVITE request** . Namely, the information needed for performing the **authentication** is included in the SIP **INVITE request** . In particular, the RAND number which is provided by an **authentication** entity (e.g., AuC or a SIP server which actually performs the authentication) has to be included...of request) may include the necessary information, namely the RAND., i.e., challenge, and information regarding the **authentication** scheme.

3S After receiving such a SIP **INVITE request** , the mobile
- 10
node responses with a SIP response like, e.g., 200 OK or the like...which is to be used by the SIP server.

5 2) The SIP server forwards the SIP **INVITE request** (containing the **authentication** extensions with the **authentication** parameters) towards the mobile node (steps S4 and S5). According to the present embodiment, the SIP server determines according to network policies that it is the **authentication** verification point. Hence, it forwards the SIP **INVITE request** with the **authentication** extensions containing only AuthDatal and puts its URL in the VIA field.

Any SIP server or proxy...the SIP INVITE request to the mobile node unchanged.

3) The mobile node (MS), receiving the SIP **INVITE request** containing the RAND parameter, executes the Z'S **authentication** algorithm taking AuthDatal as input and producing an output value AuthData2.

4) When the mobile node answers...the SIP proxy. The SIP server may determine according to network policies that it is not the **authentication** verification point. In this case, it forwards the SIP **INVITE request** with the **authentication** extensions containing AuthDatal and AuthResp.
Any SIP server or proxy receiving authentication extension with both RAND and...in this example the SIP server determines based on the network policies that it is not the **authentication** verification point, but the SIP proxy.

Hence, it forwards the **INVITE request** including AuthDatal and AuthResp to the proxy I in step S/1a.

Based on the network policies and on receiving the INVITE request includingAuthDatal and AuthResp, the SIP proxy determines that it is the **authentication** verification point. Hence, it extracts the AuthResp from the **INVITE message** and stores it. Thereafter, it forwards the INVITE request including only AuthDatal in step SS. In addition...

Claim
... parameter, the user is able to perform an authentication of the network.
Moreover, also a password based **authentication** scheme could be used. In this case, the SIP **INVITE message** as described above, some text requesting the user to type his password can be included. That is...protocol.
io

7 The method according to claim 6, wherein the session invitation message is a SIP **INVITE request** including an **authentication** header field.

8 The method according to claim 6, wherein the response message is a SIP response...protocol

21 The network system according to claim 20, wherein the session invitation message is a SIP **INVITE request** including an **authentication** header field.

22 The network system according to claim 20, wherein the response message is a SIP...35 The network control element according to claim 34, wherein the session invitation message is a SIP **INVITE request** including an **authentication** header field. 5 36. The network control element according to claim 34, wherein the response message is...protocol.

49 The subscriber equipment according to claim 48, wherein the session invitation message is a SIP **INVITE request** including an **authentication** header field.

50 The subscriber equipment according to claim 49, wherein the response

3/3,K/7 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00953079 **Image available**
AUTHENTICATION IN A COMMUNICATION SYSTEM
AUTHENTIFICATION DANS UN SYSTEME DE COMMUNICATION
Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 ESPOO, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
WESTMAN Ilkka, Keuruuntie 3-13 E 21, FIN-00510 Helsinki, FI, FI (Residence), SE (Nationality), (Designated only for: US)
NIEMI Valtteri, Tallberginkatu 3 as 43, FIN-00180 Helsinki, FI, FI (Residence), FI (Nationality), (Designated only for: US)
Legal Representative:
RUUSKANEN Juha-Pekka (et al) (agent), Page White & Farrer, 54 Doughty Street, London WC1N 2LS, FI,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200287272 A1 20021031 (WO 0287272)
Application: WO 2002IB1155 20020404 (PCT/WO IB0201155)
Priority Application: SE 200110188 20010425
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI
SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 4586

Fulltext Availability:
Detailed Description

Detailed Description
... associate with the session set-up procedures of already registered user equipment such as the so called **INVITE message** and so on may also need to be **authenticated** . The **authentication** of the session set-up request may, however,

not be required every time but may be accomplished...subscriber server (HSS) may not be
able to authenticate all session set-up requests. The HSS cannot **authenticate** e.g. all SIP **INVITE** **messages** because these messages have not necessarily been passed to' ...service attacks associated with registering messages are quickly noticed. The inventors have also found it possible to **authenticate** set-up messages such as the **INVITE** **messages** at a separate controller entity than where e.g. the registering messages are authenticated. The authentication of...needed for authentication purposes in the user 1.

The user equipment 1 checks appropriate parameters, computes an **authentication** response RES and sends the RES in an appropriate **INVITE** **message** (5.) to the P-CSCF 30. The P-CSCF forwards the message (6.) with to the S method may also be used for other purposes that for **authentication** of session initiation messages (e.g. the **INVITE** **messages**). The method can be used to **authenticate** whichever messages (e.g.

any other SIP methods) that bypasses an intermediate controller entity such as the...

3/3,K/8 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00942465
XML BASED TRANSACTION DETAIL RECORDS
ENREGISTREMENTS DE DETAILS D'OPERATIONS BASES SUR LE LANGAGE XML
Patent Applicant/Assignee:
WORLDCOM INC, 500 Clinton Center Drive, Clinton, MS 39056, US, US (Residence), US (Nationality)
Inventor(s):
GALLANT John K, 1800 Azurite Trail, Plano, TX 75075, US,
MCMURRY Kathleen A, 2991 Greenfield Drive, Richardson, TX 75082, US,
PIZZIMENTI Joseph W, 6716 Aimpoint Drive, Plano, Tx 75023, US,
Legal Representative:
GROLZ Edward W (agent), Scully, Scott, Murphy & Presser, 400 Garden City Plaza, Garden City, NY 11753, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200275605 A1 20020926 (WO 0275605)
Application: WO 2002US8578 20020320 (PCT/WO US0208578)
Priority Application: US 2001276923 20010320; US 2001276953 20010320; US 2001276954 20010320; US 2001276955 20010320; US 200299323 20020315
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI
SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 12761

Fulltext Availability:
Detailed Description

Detailed Description
... password entered as DTMF digits. As an alternate to password collection through DTMF, SCS 106 may support **authentication** using SIP. In this scenario, the SIP **INVITE** **message** carries additional user

parameters, such as usemame/password combination that may be used by SCS 106 to...

3/3,K/9 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00941946 **Image available**
SELECTIVE FEATURE BLOCKING IN A COMMUNICATIONS NETWORK
BLOCAGE SELECTIF DE CARACTERISTIQUES DANS UN RESEAU DE COMMUNICATIONS
Patent Applicant/Assignee:
WORLDCOM INC, 500 Clinton Center Drive, Clinton, MS 39056, US, US (Residence), US (Nationality)
Inventor(s):
GALLANT John K, 1800 Azurite Trail, Plano, TX 75075, US,
Legal Representative:
GROLZ Edward W (agent), Scully, Scott, Murphy & Presser, 400 Garden City Plaza, Garden City, NY 11530, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200276051 A1 20020926 (WO 0276051)
Application: WO 2002US8641 20020320 (PCT/WO US0208641)
Priority Application: US 2001276923 20010320; US 2001276953 20010320; US 2001276954 20010320; US 2001276955 20010320; US 200297592 20020315
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 11587

Fulltext Availability:
Detailed Description

Detailed Description
... back a SIP acknowledgement message to the proxy in step 505.

15
User A subsequently repeats the **INVITE request** in step 507, but this time includes an **authentication** header in response to the challenge of step 503. If the authentication of User A is satisfactory...

3/3,K/10 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00941944 **Image available**
RECURSIVE QUERY FOR COMMUNICATIONS NETWORK DATA
DEMANDE RECURSIVE DE DONNEES DE RESEAU DE COMMUNICATION
Patent Applicant/Assignee:
WORLDCOM INC, 500 Clinton Center Drive, Clinton, MS 39056, US, US (Residence), US (Nationality)
Inventor(s):
GALLANT John K, 1800 Azurite Trail, Plano, TX 75075, US,
MCMURRY Kathleen A, 2991 Greenfield Drive, Richardson, TX 75082, US,
Legal Representative:
GROLZ Edward W (agent), Scully, Scott, Murphy & Presser, 400 Garden City Plaza, Garden City, NY 11530, US,
Patent and Priority Information (Country, Number, Date):

Patent: WO 200276049 A1 20020926 (WO 0276049)
Application: WO 2002US8632 20020320 (PCT/WO US0208632)
Priority Application: US 2001276923 20010320; US 2001276953 20010320; US 2001276954 20010320; US 2001276955 20010320
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 14394

Fulltext Availability:
Detailed Description

Detailed Description
... back a SIP acknowledgement message to the proxy in step 305.

[00721 User A subsequently repeats the **INVITE request** in step 307, but this time includes an **authentication** header in response to the challenge of step 303. If the authentication of User A is satisfactory...

3/3,K/11 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00920593 **Image available**
VOIP TERMINAL SECURITY MODULE, SIP STACK WITH SECURITY MANAGER, SYSTEM AND SECURITY METHODS
MODULE DE SECURITE D'UN TERMINAL VOIP, PILE SIP DOTE D'UN GESTIONNAIRE DE SECURITE, SYSTEME ET PROCEDES DE SECURITE
Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality)
NOKIA INC, 6000 Connection Drive, Irving, TX 75039, US, US (Residence), US (Nationality), (Designated only for: LC)
Inventor(s):
NUUTINEN Mikko, Servin Maijantie 12 i 131, FIN-02150 Espoo, FI,
Legal Representative:
MAGUIRE Francis J (agent), Ware, Fressola, Van Der Sluys & Adolphson LLP, 755 Main Street, P.O. Box 224, Monroe, CT 06468, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200254704 A2-A3 20020711 (WO 0254704)
Application: WO 2001IB1700 20010918 (PCT/WO IB0101700)
Priority Application: US 2000752142 20001229
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 12762

Fulltext Availability:
Detailed Description

Detailed Description
... stack, where the message is received, identified and sent, is modified to handle all the security messages. **Invite messages** and **authentication** related response messages are always sent to security manager. In practice, this means that the authentication is...

3/3,K/12 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00904257 **Image available**
MEDIA BINDING TO COORDINATE QUALITY OF SERVICE REQUIREMENTS FOR MEDIA FLOWS IN A MULTIMEDIA SESSION WITH IP BEARER RESOURCES
LIAISON DE MEDIAS AFIN DE COORDONNER LES EXIGENCES EN MATIERE DE QUALITE DE SERVICE POUR DES FLUX DE MEDIAS DANS UNE SESSION MULTIMEDIA AVEC DES RESSOURCES DE SUPPORT IP
Patent Applicant/Assignee:
TELEFONAKTIEBOLAGER LM ERICSSON (publ), S-126 25 Stockholm, SE, SE (Residence), SE (Nationality)
Inventor(s):
FOTI George, Dollard des Ormeaux, 163 Mozart, Quebec, H9G 2Z8, CA,
OYAMA Johnson, c/o Robertsson, Forngrand 1 3tr, S-169 68 Solna, SE,
SURDILA Sorin, 463 Toussaint, St. Dorothee, Laval, Quebec H7X 3N3, CA,
WIDEGREN Ina Birgitta, Heleneborgsgatan 25C 1tr, S-117 31 Stockholm, SE,
WILLIAMS Brian Charls, 11 St. Georges Crt,, Greensborough, VIC 3080, AU,
Legal Representative:
MAGNUSSON Monica (agent), Ericsson Radio Systems AB, Patent Unit Radio Access, S-164 80 Stockholm, SE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200237753 A2-A3 20020510 (WO 0237753)
Application: WO 2001SE2446 20011106 (PCT/WO SE0102446)
Priority Application: US 2000246501 20001106; US 2000248110 20001113; US 2001273678 20010306; US 2001985573 20011105
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI
SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 14643

Fulltext Availability:
Detailed Description

Detailed Description
... relating to each of the medias being requested for the session. The proxy-CSCF-A forwards the **INVITE message** to UE-A's serving CSCF-A which **authenticates** UE-A and authorizes the multimedia call. The **INVITE message** is then forwarded to the B side through UE-B's serving-CSCF-B to UE-B...

3/3,K/13 (Item 11 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00877862 **Image available**

TECHNIQUES FOR PERFORMING UMTS-AUTHENTICATION USING SIP (SESSION INITIATION PROTOCOL) MESSAGES

TECHNIQUES D'EXECUTION D'AUTHENTIFICATION UMTS (SYSTEME UNIVERSEL DE TELECOMMUNICATIONS DU SERVICE MOBILE) AU MOYEN DE MESSAGES SIP (PROTOCOLE D'INITIATION DE SESSION)

Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
FACCIN Stefano, 3421 Dartmoor, Dallas, TX 75229-2622, US, US (Residence), IT (Nationality), (Designated only for: US)
LE Franck, 2715 West Royal Lane #212, Irving, TX 75063, US, US (Residence), FR (Nationality), (Designated only for: US)
WOLFNER Gyorgy, Szepvolgyi ut 4a, H-1025 Budapest, HU, HU (Residence), HU (Nationality), (Designated only for: US)
Legal Representative:
BRUNDIDGE Carl I (et al) (agent), Antonelli, Terry, Stout & Kraus, LLP, Suite 1800, 1300 North Seventeenth Street, Arlington, VA 22209, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200211469 A2-A3 20020207 (WO 0211469)
Application: WO 2001US23764 20010730 (PCT/WO US0123764)
Priority Application: US 2000630425 20000801
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 3011

Fulltext Availability:
Detailed Description

English Abstract

...an SIP request from the user agent to the server. The server then forwards a request for **authentication** to the user agent in response to the **invite request** , the request for **authentication** including information that the **authentication** will be performed using a UMTS AKA mechanism. The user agent then forwards and authentication response to...

...response to the SIP request. The SIP request may include any standardized SIP request including an SIP **INVITE request** or an SIP REGISTER request. The request for **authentication** may include one of an SIP 401 Unauthorized code or an SIP 407 Proxy Authentication Required code...

Detailed Description

... MAC (Message Authentication Code) is considered to be invalid).

Referring now to Figure 2, which illustrates proxy **authentication** after an **INVITE request** is presented, upon the UA forwarding an **INVITE request** to the CSCF, the CSCF may ask for an **authentication** with a 407 Proxy Authentication Required response. The 407 responds contains a Proxy-Autbenticate response header field...

...parameters.

After receiving the 407 response, the UA sends an ACK (acknowledgment) response and may repeat the **INVITE request** , the repeated request containing the appropriate **authentication** information in the Proxy-Autborization header field.

4
In the case of the UMTS AKA procedure,theProxy...

...challenge) and the AUTN (authentication token).
After a 401 response, the UE a sends a new REGISTER/ **INVITE request** which
should contain the appropriate **authentication** information in the Authorization header field: the authentication response (RES), a synchronization failure parameter (AUTS), or an...

3/3,K/14 (Item 12 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00844671 **Image available**
METHOD AND APPARATUS FOR S.I.P./H.323 INTERWORKING
PROCEDE ET DISPOSITIF POUR INTERFONCTIONNEMENT S.I.P./H.323
Patent Applicant/Assignee:
AT & T CORPORATION, 32 Avenue of the Americas, New York, NY 10013-2412, US, US (Residence), US (Nationality)
Inventor(s):
AGRAWAL Hemant, Shivam Electro Platers, Mathura 281 001, Uttar Pradesh, IN,
PALAWAT Vipin, Apt. 11, 74 Branch Street, Lowell, MA, US,
ROY Radhika R, 14 Derringer Drive, Howell, NJ 07731, US,
Legal Representative:
DWORETSKY Samuel H (et al) (agent), AT & T Corp, P.O. Box 4110, Middletown, NJ 07748-4110, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200178347 A2-A3 20011018 (WO 0178347)
Application: WO 2001US11451 20010409 (PCT/WO US0111451)
Priority Application: US 2000195937 20000410; US 2001825304 20010404
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
CA MX
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
Publication Language: English
Filing Language: English
Fulltext Word Count: 8116

Fulltext Availability:
Detailed Description

Detailed Description
... support simple call supplementary services like call forwarding, call hold and call transfer, conferencing, session change (re- **invite** , mode **request**), security: **Authentication** , Authorization and privacy,. quality of service QOS) signaling, network management and redundancy.

[77] Now, we will discuss...

3/3,K/15 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00805810 **Image available**
INTERNET PROTOCOL TELEPHONY VOICE/VIDEO MESSAGE DEPOSIT AND RETRIEVAL
DEPOT ET RETRAIT DE MESSAGE VOCAL/VIDEO DE TELEPHONE INTERNET
Patent Applicant/Assignee:
MCI WORLDCOM INC, 515 East Amite Street, Jackson, MS 39201, US, US (Residence), US (Nationality)
Inventor(s):
DONOVAN Steven R, 704 Forest Bend Drive, Plano, TX 75025, US,
Legal Representative:

GROLZ Edward W (agent), Scully, Scott, Murphy & Presser, 400 Garden City Plaza, Garden City, NY 11530, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200139441 A1 20010531 (WO 0139441)

Application: WO 2000US41985 20001108 (PCT/WO US0041985)

Priority Application: US 99436795 19991108

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 5771

Fulltext Availability:

Detailed Description

Detailed Description

... voiceinail @sip.wcom

com>

Callid: 123456@caUing-host.com

CSeq: I ACK

Content-Length: 0

The SIP **INVITE** **request** above contains the account information, with no

password **authentication** . At this point, the IMS 25 prompts the calling IMS account user for a password to verify...

...CSeq: I ACK

Content-Length: 0

In this case, the SIP RMTE request contains no account or **authentication**

information, but only the identifier UNKNOWN in the **INVITE** **request** URL.

Accordingly, in step 395, a calling party is prompted for a user name and password. If...

```
File 275:Gale Group Computer DB(TM) 1983-2005/Mar 10
         (c) 2005 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2005/Mar 10
         (c) 2005 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2005/Mar 10
         (c) 2005 The Gale Group
File  16:Gale Group PROMT(R) 1990-2005/Mar 10
         (c) 2005 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2005/Mar 10
         (c)2005 The Gale Group
File 624:McGraw-Hill Publications 1985-2005/Mar 10
         (c) 2005 McGraw-Hill Co. Inc
File  15:ABI/Inform(R) 1971-2005/Mar 10
         (c) 2005 ProQuest Info&Learning
File 647:CMP  Computer Fulltext 1988-2005/Feb W3
         (c) 2005 CMP Media, LLC
File 674:Computer News Fulltext 1989-2005/Mar W1
         (c) 2005 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2005/Mar 09
         (c) 2005 The Dialog Corp.
File 369:New Scientist 1994-2005/Feb W4
         (c) 2005 Reed Business Information Ltd.
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 610:Business Wire 1999-2005/Mar 10
         (c) 2005 Business Wire.
File 613:PR Newswire 1999-2005/Mar 10
         (c) 2005 PR Newswire Association Inc

Set     Items   Description
S1      38893   SIP OR SESSION()(INITIATION OR INITIATED)()PROTOCOL
S2         65   INVITE(1W)(REQUEST? ? OR MESSAGE? ?)
S3          0   S2(10N)AUTHENTICAT?
S4          0   S2(30N)AUTHENTICAT?
```

```
File   8:Ei Compendex(R) 1970-2005/Feb W4
         (c) 2005 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2005/Feb
         (c) 2005 ProQuest Info&Learning
File  65:Inside Conferences 1993-2005/Mar W1
         (c) 2005 BLDSC all rts. reserv.
File   2:INSPEC 1969-2005/Feb W4
         (c) 2005 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2005/Jan W4
         (c)2005 Japan Science and Tech Corp(JST)
File 483:Newspaper Abs Daily 1986-2005/Mar 05
         (c) 2005 ProQuest Info&Learning
File   6:NTIS 1964-2005/Feb W4
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2005/Feb W4
         (c) 2005 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Mar W1
         (c) 2005 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Jan
         (c) 2005 The HW Wilson Co.
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 266:FEDRIP 2005/Jan
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2005/Jan W5
         (c) 2005 FIZ TECHNIK
File 438:Library Lit. & Info. Science 1984-2005/Jan
         (c) 2005 The HW Wilson Co

Set     Items   Description
S1       9557   SIP OR SESSION()(INITIATION OR INITIATED)()PROTOCOL
S2         11   INVITE(1W)(REQUEST? ? OR MESSAGE? ?)
S3          0   S2(10N)AUTHENTICAT?
S4          0   S2 AND AUTHENTICAT?
```